GATES

SUPPORTING STATEMENT – PART A

A. JUSTIFICATION

1. Need for the Information Collection

The Global Air Transportation Execution System (GATES) collects information from the public to support the following: Aerial Ports and Water Ports of Embarkation and Debarkation; Military Transportation Offices; Air Mobility Support Flights; Passenger Gateways; Navy Operated Air Terminals and Aerial Ports; SDDC Army and Navy Water Ports; Military airfields or installations (all services); any activity or agency responsible for initiating or receiving a request for movement of personnel and their baggage, manifesting, tracing, billing actions, or statistical data collection; and deployed fixed and non-fixed airfields throughout the world. Passenger records are used to prepare aircraft manifests for passenger identification processing and movement on military aircraft, commercial contract (charter) aircraft, and on seats reserved (blocked) on regularly scheduled commercial aircraft at military and civilian airports. Records containing data in this system are also used to: (a) develop billing data to the user Military Services or other organizations; (b) determine passenger movement trends; (c) forecast future travel requirements; (d) identify, research, and resolve transportation related problems; and, (e) screening for customs, immigration, and transportation security purposes.

Legal or administrative requirements that mandate the collection of data are;

Defense Transportation Regulation 4500.9-R (Part I, Chapter 103, Section N), The Defense Transportation Regulation; Department of Defense Instruction 4500.57 (Enclosure 3, Paragraph 3.4), Transportation and Traffic Management; Air Force Instruction 24-101 (Chapter 1, Section 1.11), Passenger Movement; Air Mobility Command Instruction 24-101 (Volume 14, Section E, Paragraph 36), Military Airlift Passenger Service; Chief of Naval Operations Instruction 4650.15 (Paragraph 5.c.), Navy Passenger Transportation Manual; Marine Corps Order P4600.7 (Appendix A), Marine Corps Transportation Manual; Army Regulation 700-80 (Chapter 2-1), Army In-Transit Visibility; Code of Federal Regulations, Title 14, (Part 243), Passenger Manifest Information; Code of Federal Regulations, Title 49, (Part 175), Carriage by Aircraft; Code of Federal Regulations, Title 49, (Part 1540), Civil Aviation Security: General Rules; Code of Federal Regulations, Title 49, (Part 1544), Aircraft Operator: Security: Air Carriers and Commercial Operators; Joint Federal Travel Regulations, Joint Travel Regulations Travel and Transportation Reform Act of 1998, Public Law 105-264 (Section 2); United States Code, 49 U.S.C. (§ 41113), Aviation Disaster Family Assistance Act of 1996; and United States Code, 49 U.S.C. (§ 44903), Air Transportation Security.

2. Use of the Information

GATES collects data for passenger manifests for travelers using government conveyances boarding at aerial ports worldwide. Travelers using government conveyances

provide data in person, via e-mail, and/or paper based collections to port personnel. Data must be collected to execute USTRANSCOM missions. data is used to: 1) prepare aircraft manifests for passenger identification processing and movement on military aircraft, commercial contract (charter) aircraft, and on seats reserved on regularly scheduled commercial aircraft at military and civilian airports; 2) screen passengers for customs, immigration, and transportation security purposes; and, 3) create manifests and records relating to the movement of personal property and human remains.

The use of data collected in GATES allows for developing billing data for use by the user Military Services or other organizations; manifest human remains; determine passenger movement trends; forecast future travel requirements; identify, research, and resolve transportation-related problems; notify foreign countries of personnel and equipment arrivals; manifest passengers; screen passengers for customs, immigration, and transportation security purposes; and, manifest and create records relating to the transportation of personal property and human remains.

Automated and manual transfers of data can occur between GATES and other systems through a Memorandum of Agreement. Data can also be embedded in the transportation control number for personal property shipments and for supercargo. GATES has collected data previously for passenger manifests.

3. Use of Information Technology

Travelers using government conveyances provide data in person via check-in prior to boarding the aircraft, via e-mail, and/or paper based collections to port personnel. Automated and manual transfers of data can occur between GATES and other systems. Paper-based collection represents 15% of data collected.

4. Non-duplication

Information is not already available therefore the traveler must provide this information to verify and identify who they are prior to boarding an aircraft.

5. Burden on Small Business

Not applicable.

6. Less Frequent Collection

The collection of data is voluntary; however failure to provide the information could result in the individual and/or personal property not being accepted for transportation.

7. Paperwork Reduction Act Guidelines

No special circumstances exist that would not adhere to the guidelines in 5 CFR 1320.5.

8. Consultation and Public Comments

a. 60-day Federal Register Notice was published on 8 April 2014 2014 (79 FR 19321). Public comment ended on 6/8/2014 and no comments were received.

9. Gifts or Payment

Not applicable.

10. Confidentiality

Confidentiality ensures that only those personnel with the appropriate security clearance and the need-to-know shall be allowed access to data processed, handled or stored on system components. Confidentiality targets the protection of information from unauthorized access. Personnel, physical and administrative security mechanisms applied to the system shall minimize risks of unauthorized disclosure of command and control information.

GATES policy references are:

- DoDD 5205.2, DoD Operations Security (OPSEC) Program, 20 June 2012.
- DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
- DoDI 8500.01, Cybersecurity, 14 March 2014
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014

The GATES Information System Security Policy implements Air Force Policy Directive (AFPD) 33-2, Information Assurance (IA) Program and Air Force Instruction (AFI) 33-200, Information Assurance (IA) Management. It consolidates and clarifies the direction/guidance contained in Department of Defense (DoD) and Air Force security publications. This security policy applies to all personnel involved with the development, maintenance and operation of an automated information system Users shall ensure sensitive-but-unclassified materials, which require special marking and handling such as For Official Use Only (FOUO), mandated by the Freedom of Information Act (FOIA) or Privacy Act (PA), are marked in accordance with DoDM 5200.01-V4, DoD Information Security Program: Controlled Unclassified Information (CUI).

DoDI 8500.01, enclosure 3, paragraph 8 states that access to all DoD information systems (i.e., workstations, computers, servers, etc.) ensure strong identification and authentication so that entities' access and access behavior are visible, traceable, and enable continuous monitoring for law enforcement and cybersecurity. DODI 8500.01 paragraph 3i(1) also states the cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with this instruction and adherence to DoD 5200.2-R, paragraph 3.6.15 and Federal Information Processing Standards (FIPS) Publication 201-1 which further implements Homeland Security Presidential Directive (HSPD) 12 for specific clearance/investigation requirements. The minimum investigation required for GATES access is a National Agency Check with Inquiries (NACI) or host nation equivalent of a NACI.

DoDI 8500.01, enclosure 3, paragraph 11c(2) states that access must be strictly limited to information that has been cleared for release. GATES data is considered For Official Use Only (FOUO). GATES implements role-based security controls for user access deemed necessary to meet their mission. Interface partners require approved written requirements for specified data only.

DoDI 8500.01, enclosure 3, paragraph 10 requires all users of DoD information systems must be adequately trained to perform their information assurance responsibilities. Information Assurance Training shall be accomplished and documented for all personnel prior to their obtaining system access. Training will consist of the applicable requirements contained as stated above and local security procedures. DoD 8570.01-M shall be met by all GATES users with privileged access.

DoDI 8500.1, enclosure 3, paragraph 7i, requires data must be protected in accordance with DoD 4500.11-R when processed or stored. Users are responsible for protecting and safeguarding all sensitive information under their control. Sensitive information includes, but is not limited to, privacy act data, privileged data, proprietary data, logistics records, procurement data, financial data, investigative data, auditor records, For Official Use Only data, scientific and technical data (which has national security related implications), unit mobility or deployment information. The computing facility where data is stored enforces restrictive access features. The Consolidated Computing Facility located on Scott AFB and Defense Enterprise Computing Center (DECC) St Louis, MO require privileged keycard entry. Access to both facilities require authentication of identification documents for review by security forces for entry.

Users are responsible for protecting and safeguarding all sensitive information under their control. Sensitive information includes, but is not limited to, privacy act data, privileged data, proprietary data, logistics records, procurement data, financial data, investigative data, auditor records, For Official Use Only data, scientific and technical data (which has national security related implications), unit mobility or deployment information, and classified information. Also, the aggregation of unclassified information may result in the creation of sensitive data. Use the following guidelines on how to protect sensitive information.

- Do remove compact disc containing sensitive information from your computer and properly store them when they are no longer being used.
- Do store compact disc containing sensitive-but-unclassified information in locked offices or in a locked storage container during non-duty hours.
- Do properly safeguard, store and dispose of sensitive information.
- Do ensure all classified papers contain the date of creation, the highest classification level of the data contained in the document, the downgrading instructions or review date, and the name of the originator.
- Do when possible; use internal markings on files to indicate the type of sensitive data contained in the file and any special handling instructions.
- Do dispose of computer products containing sensitive-but-unclassified information in accordance with the records disposition schedule that is available on the AF Records Information Management System (AFRIMS) website.
- Do not place sensitive-but-unclassified data on diskettes used for general correspondence.
- Do not provide sensitive information to an individual until you have determined he or she has a valid need-to-know requirement for the information as part of their official duties.

Information Assurance Training shall be accomplished and documented for all personnel prior to their obtaining system access. Training will consist of the applicable requirements contained in AFI 33-115 Volume 2, Licensing Network Users and Certifying Network Professionals, this policy and local security procedures.

The Privacy Act System of Records Notice (SORN) ID number is FO24 AF USTRANSCOM D DoD, Defense Transportation System Records. .

The GATES Privacy Impact Assessment dated November 2011 resides at URL https://www.ustranscom.mil/FOIA/PIA.CFM and is currently being updated to include additional information.

In accordance with DoDD 5400.11 there is no violation of the DoD Privacy Program. The Privacy Act Statement is included in the application for air travel AMC Form 140 for individuals requesting travel. Reference AMCI24-101V14 page 10 paragraph 2.10, a Privacy Act Statement is displayed for the applicants at all the GATES passenger terminals for the collection of personal information. If an individual objects, the Privacy Act Statement informs them that failure to provide the information could result in them not being accepted for travel on military aircraft.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. See GRS 20, 12b. (N1-GRS-95-2 item 12b)

11. Sensitive Questions

The justification for use of the social security number is dated 7 December 2011. The Defense Transportation Regulation (DTR) – Part I, Chapter 103, page 19-20, provides guidance for managing passenger movements (manifests). IAW with this guidance, Traveler Identification Social Security Number is mandatory. Specifically, passenger manifesting systems and procedures must collect at a minimum passenger name, rank, SSN or passport number, status (e.g., active, reserve, retired, dependent, civilian), sponsoring agency, and emergency contact (e.g., name, telephone number of person not traveling with individual). The DTR – Part II, provides guidance for managing personal property movements (manifests) and the member/employee SSN is mandatory (Part II, Appendix L, page II-L-6. Reference attached SSN justification letter attached.

The Privacy Act Statement is included in the AMC Form 140 (Application of Air Travel; Space Available Travel Request) and is provided to each passenger for completion. After the passenger is manifested in GATES, one copy of the AMC Form 140 is shredded by the passenger terminal personnel. The passenger terminal personnel then annotate the traveler's date/time of sign-up on the second copy and return it to the traveler. GATES database contains the passenger information and is maintained for ten years for metrics or reporting purposes after which the data is purged out of the historical database. (AMC Form 140) Per AMCI 24-101V14 page 10 paragraph 2.10, the following privacy act statement displays for the applicants at all the GATES passenger terminals: “DISCLOSURE is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request”.

5 U.S.C. § 552a(b)(3) (routine uses) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D).

12. Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden.

Number of respondents: 184,589
Number of responses per respondents: 1
Total Annual Responses: 184,589
Annual burden hours: 15,382
Average burden per response: 5 minutes

b. Labor Cost of Respondent Burden

Estimated hourly rate: 37.92
Rate Per Response: 3.16
Total Labor Cost: 583,301

13. Respondent Costs Other Than Burden Hour Costs

$0

14. Cost to the Federal Government

Software development costs incurred to allow for the collection and transmission of the data is $500K. Annual operations and maintenance costs are $50K. Cost to government

Estimated hourly rate: 17.26
Average burden per response: 2 mins
Total Cost to Gov't: 106,183

TOTAL ANNUAL COST TO GOVT: $156,183

15. Reasons for Change in Burden

This collection was changed based on a mandate from the Office of Secretary of Defense and based on Federal Register Volume 78, Number 175, Department of Homeland Security (DHS) Transportation Security Administration (TSA) 019 Secure Flight Records System of Records. This is a new collection, already in existence, with new burden.

16. Publication of Results

Not applicable.

17. Non-Display of OMB Expiration Date

Not applicable.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

Not applicable.